1. How is accessing the web server through the VPN different than the port forwarding method we used in prior labs? (HINT: think about the IP address you used to access the web server in each case)
   1. Assume we upgraded the webserver to support https - which method is a more secure method to access the web server? Why?
2. What type of VPN deployment architecture does this represent?
   1. HINT: think about the rules that got created during the VPN server wizard
3. Go back through the settings for the VPN Server that you created in pfSense. Locate the “Tunnel Settings” area.
   1. What setting could you change to make sure we don’t create a split tunnel on the client workstation when they connect?
4. Using the pfSense book, go through the OpenVPN chapter and answer the following questions
   1. What protocol does OpenVPN use for encryption/tunneling?
   2. What types of authentication can OpenVPN utilize?
5. Based on the recommendations in Chapter 11 of the textbook, list another configuration change or feature you would like to implement – Can OpenVPN support it?